[Insert Cover Picture]

Cruise Ship Incident Tabletop Exercise

Situation Manual

[Insert Date]

\*[Insert Caveat]\*

This Situation Manual (SitMan) provides exercise participants with all necessary tools for their roles in the exercise. Some exercise material is intended for the exclusive use of exercise planners, facilitators, and evaluators, but players may view other materials that are necessary to their performance. All exercise participants may view the SitMan.

This page is intentionally left blank.

# Exercise Agenda

| Start Time | End Time | Activity |
| --- | --- | --- |
| 7:45 AM | 8:30 AM | Registration |
| 8:30 AM | 8:45 AM | Welcome and Introductions |
| 8:45 AM | 9:45 AM | Module One: Pre-Incident Phase |
| 9:45 AM | 9:55 AM | Break |
| 9:55 AM | 10:55 AM | Module Two: Incident and Response Phase |
| 10:55 AM | 11:05 AM | Break |
| 11:05 AM | 12:05 PM | Module Three: Recovery Phase |
| 12:05 PM | 12:30 PM | Hot Wash / Closing Remarks |

*\*All times are approximate*

This page is intentionally left blank.

# Exercise Overview

|  |  |
| --- | --- |
| **Exercise Name** | Cruise Ship Incident Tabletop Exercise (TTX) |
| **Exercise Dates** | [Indicate the start and end dates of the exercise] |
| **Scope** | This exercise is a TTX planned for [insert exercise duration] and will focus on [insert scope].This exercise was developed using materials created by the Cybersecurity and Infrastructure Security Agency (CISA) for a CISA Tabletop Exercise Package (CTEP). |
| **Mission Area(s)** | Prevention, Protection, Mitigation, Response, and Recovery [Select appropriate Mission Areas] |
| **Capabilities** | * Economic Recovery
* Infrastructure Systems
* Intelligence and Information Sharing
* On-scene Security, Protection, and Law Enforcement
* Operational Communications
* Operational Coordination
* Planning
* Public Information and Warning
* Situational Assessment
 |
| **Objectives** | 1. Examine response and recovery plans and procedures following a drone attack.
2. Discuss information sharing procedures and communication and coordination protocols between private and local public sector partners.
3. Examine company and port security short-term recovery plans.
4. [Insert additional exercise objectives as necessary]
 |
| **Threat or Hazard** | Drone / Improvised Explosive Device (IED) |
| **Scenario** | A radical environmental group has launched a swarm drone attack against a docked cruise ship seeking to damage navigational systems to stop cruise ship operations. |
| **Sponsor** | [Insert the name of the sponsor organization, as well as any grant programs being used, if applicable] |
| **Participating Organizations** | [Please see Appendix A.] |
| **Point of Contact** | [Insert the name, title, agency, address, phone number, and email address of the primary exercise point of contact (POC) (e.g., exercise director or exercise sponsor).] |

# General Information

## Exercise Objectives and Capabilities

The exercise objectives in Table 1 describe the expected outcomes for the exercise. The objectives are linked to capabilities, which are the means to accomplish a mission, function, or objective based on the performance of related tasks, under specified conditions, to target levels of performance. The objectives and aligned capabilities are guided by senior leaders and selected by the Exercise Planning Team (EPT).

| **Exercise Objectives** | **Capability** |
| --- | --- |
| Examine response and recovery plans and procedures following a drone attack. | * Infrastructure Systems
* Intelligence and Information Sharing
* On-scene Security, Protection, and Law Enforcement
* Operational Communications
* Operational Coordination
* Planning
 |
| Discuss information sharing procedures and communication and coordination protocols between private and local public sector partners. | * Intelligence and Information Sharing
* Operational Communications
* Operational Coordination
* Planning
* Public Information and Warning
* Situational Assessment
 |
| Examine company and port security short-term recovery plans.  | * Economic Recovery
* Public Information and Warning
* Operational Coordination
 |
| [Insert additional objectives as necessary.] | * [Insert additional core capabilities as necessary.]
 |

Table 1. Exercise Objectives and Associated Capabilities

## Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

* **Players** have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.
* **Observers** do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.
* **Facilitators** provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key EPT members also may assist with facilitation as subject matter experts (SMEs) during the exercise.
* **Moderators** are responsible for admitting and signing in all participants to the virtual exercise, monitoring the chat area for questions and / or issues, and controlling participant audio.
* **Date Collectors** are assigned to observe and document the discussion during the exercise, participate in data analysis, and assist with drafting the After-Action Report (AAR).

## Exercise Structure

This exercise will be a discussion-based, facilitated exercise. Players will participate in the following three modules:

* Module One: Pre-Incident
* Module Two: Incident and Response
* Module Three: Recovery

Each module begins with a multimedia update that summarizes key events occurring within that time period. After the updates, participants review the situation and engage in discussions of appropriate [insert mission area] issues.

## Exercise Guidelines

* This exercise will be held in an open, no-fault environment wherein capabilities, plans, systems, and processes will be evaluated. Varying viewpoints, even disagreements, are expected.
* Respond to the scenario using your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from your training.
* Decisions are not precedent setting and may not reflect your jurisdiction’s / organization’s final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions.
* Issue identification is not as valuable as suggestions and recommended actions that could improve [insert mission area] efforts. Problem-solving efforts should be the focus.
* The assumption is that the exercise scenario is plausible, and events occur as they are presented. All players will receive information at the same time.

## Exercise Evaluation

Evaluation of the exercise is based on the exercise objectives and aligned core capabilities. Players will be asked to complete a participant feedback form. These documents, coupled with facilitator observations and evaluator notes, will be used to evaluate the exercise and then compiled into the AAR / Improvement Plan (IP).

This page is intentionally left blank.

# Module One: Pre-Incident Phase

## Scenario

## [Insert Location]

### [Insert Month, Day, Year]: [Insert Time]

While pulling into [enter domestic location] port, the [insert ship name] cruise ship holding over 6,000 passengers, encountered a large, non-violent demonstration at the port protesting the cruise ship industry. At approximately 1:35 p.m., a radical environmental group, [insert group name], staged a sit-in outside of the security barrier at the port. Over 200 protestors attended the demonstration and were screaming at passengers and crew members urging them to sign their petitions.

The demonstration lasted about 2.5 hours and the passengers, port personnel, and ship crew members largely ignored the protestors, leading the protestors to grow louder and more hostile. As the demonstrators grew more volatile, many protestors attempted to jump the barrier and charge the ship.

Port personnel sprang into action and were able to secure the barrier but still had to call local police to disperse the crowd. Police arrested four of the group’s leaders because they resisted arrest and threatened to kill crew members and police officers.

Aside from a short article in a local newspaper, the demonstration went largely unnoticed despite weeks of planning by the group’s leadership.

After their release from jail, one of the group’s leaders posted on the group’s social media page stating their fight against the cruise industry had only just begun. The post claimed they were going to continue until they “made the cruise industry suffer in the same way they had made the region suffer.”

## Discussion Questions

1. What formal information sharing processes would your organization use at this point?
	1. Would you send out messages to employees? The public?
	2. Would you send any messaging out for non-credible threats?
2. What resources do you use to disseminate information?
	1. What notification capabilities (e.g. alerts, email, telecom, text message, etc.) do you use to share information and communicate protective measures?
3. What measures would on-board security take at this time to protect your organization?
4. How is your organization coordinating with information sharing partners, such as the Department of State, Federal Bureau of Investigation (FBI), Customs and Border Protection (CBP), fusion centers, and local law enforcement?
5. What training regarding dealing with protests is available to employees?
	1. Is the training mandatory?
	2. Does the training instruct employees in documenting and reporting aggressive behavior?
	3. Does it include information and protocols for addressing protests in a port?
	4. Do employees know who to contact with questions and concerns relating to outsider threats?
6. Should crew and port authority take any action after witnessing this incident?
	1. Are plans or procedures available to guide employees in their actions / decisions?
	2. Is there a system for collaboration between the cruise line and port security?
7. As the security officer, should you interview passengers and crew after they pass by the protestors?
	1. After leaving the port, should the captain reach out to passengers to discuss the protest?
8. What actions, if any, should the ships’ leadership take to protect the safety of passengers and crew?
	1. What actions could crew members or port personnel have taken to reduce disruptive, threatening, or potentially violent behaviors?
		1. Should port personnel have reported the protestors’ behavior to security earlier? Should someone have called the local authorities prior to the attempted security breach?
	2. Did any of the crew’s or port authority’s actions potentially increase the outcome of violence?
9. Are port / company policies adequate to de-escalate this from becoming a violent incident? Are there any ways decision makers could improve these policies?

# Module Two: Incident and Response Phase

## Scenario

## [Insert Location]

### [Insert Previous Date + 1 Day]: [Insert Time]

At approximately 11:15 a.m., the [insert ship name] cruise ship is pier side at [enter domestic location] port and most passengers have disembarked the ship to go about their planned activities. The [insert ship name] cruise ship is the largest of the fleet, holding over 6,000 passengers, most of whom are United States citizens.

The crew is going about their regular duties and port security personnel are at their appropriate posts. One crew member is taking the poolside bar’s inventory when they hear a loud buzzing sound. They look up and see approximately eight drones rapidly advancing towards the ship. The crew member runs to the nearest phone to call the bridge and inform the ship’s captain and security officer.

Moments later, passengers can hear loud bangs coming from the top of the ship where the navigation equipment is housed. A small explosion occurs at the base of the navigational equipment, partially destroying the equipment. The ship also incurs some superficial damage from the blast.

Those aboard can hear the explosion throughout the ship, and crew members immediately alert the captain who goes to the bridge to further investigate. All but two drones have flown away after dropping IEDs on the ship. The two remaining drones are circling the ship and hovering near the communications equipment. They appear to be conducting surveillance.

On the ground, port security personnel see the drone attack and immediately shut down the port and call local authorities.

Minutes later, aboard the ship, the captain is delegating the security team to search the ship for any injured passengers or crew members. The captain uses the ship’s wide public address (PA) system to inform everyone aboard that there has been an incident on the ship. The captain has issued a shelter-in-place order for all passengers and crew. The staff captain is on the phone with shore-side security alerting them to the situation at hand.

At 11:40 a.m., local law enforcement arrives at the port. They quickly establish their own command post, receive a debrief from the ship’s security officer, and hurry aboard the ship. Once on the ship, local law enforcement, along with ship security, head to the rooftop deck to further assess the damage and care for any injured people. The drones immediately fly off when they see local law enforcement.

## Discussion Questions

1. Do the ship’s incident response plans (e.g., ship security plans, emergency action plans, emergency response plans, or other appropriate plans) contain protocols for responding to a drone attack?
	1. Have employees trained for this type of emergency incident?
		1. Is emergency contact information made available at all phones?
		2. What procedures exist for sheltering-in-place and evacuation?
	2. Does ship personnel advise passengers on how to respond during this (or any) emergency incident?
	3. Does the security team have notification systems to warn crew and passengers both on- and off-site during such an incident?
	4. How do you communicate with crew and passengers during an incident?
		1. Have you established a protocol for how to contact tour operators following an incident?
	5. What instructions will your organization give to the crew and passengers (e.g., evacuation, shelter-in-place, lockdown)?
	6. Is there a way to account for crew / passengers? (i.e., those who went ashore / those who stayed aboard)?
	7. Are there any critical operations on the ship that your organization must secure for safety reasons? If so, do procedures exist for doing so in an emergency?
	8. What other life safety issues should your organization consider?
2. What does your on-board security team look like?
	1. How has your organization trained security to respond to this type of incident? What are their roles and responsibilities?
	2. Do security personnel and first responders have interoperable radios / communication? Do plans exist for first responders to communicate if they cannot communicate via radio?
	3. Is security clearly identifiable upon arrival of law enforcement?
3. Does your company have information and protocols for addressing physical threats from outsiders?
	1. Have security personnel equipped the ship to detect drones?
	2. If so, are there capabilities to disarm a drone?
4. Is your company familiar with federal resources available for consultation once a threat management team opens a case, such as the U.S. Secret Service (USSS) National Threat Assessment Center?
	1. With what organizations would you communicate (e.g., local law enforcement agencies, FBI, CBP, Department of State)?
	2. Does your organization maintain a relationship with your Department of Homeland Security (DHS) Protective Security Advisor (PSA)? If so, do you have a rapid means of contacting them?
	3. Does your organization use the Homeland Security Information Network – Critical Infrastructure (HSIN–CI) portal?
5. Is there training for the crew on how to handle emergencies in a domestic port of call?
	1. How would the crew work side by side with local first responders?
	2. How would they handle large cultural / language barriers?
	3. How would the crew handle such an incident in a country with limited resources / infrastructure?
6. Do the ships have physical security measures that may be relevant to this scenario?
7. What types of perimeter security does the port / ship have (e.g., fences, doors, gates)?
8. What types of vehicle control checkpoints are present at the port? (e.g., barriers, driveways, parking lots)?
9. How do different ports all over the world coordinate the emergency response?
	1. Does the ship provide any of its incident response plans (e.g., site security plans, emergency action plans, emergency response plans, or other appropriate plans) to first responders in preparation for potential incidents?
		1. If so, are the incident response plans available in more than one language?
		2. If not, how do responders communicate key information during the response to those who may not speak the same language?
	2. How do emergency response personnel access the ship?
		1. Upon arrival of law enforcement, is there a “go bag” available to them containing desired items such as ship floor plans, access swipe cards, elevator keys, etc.?
	3. Are there any safety concerns for first responders that your organization needs to address (e.g., entering restricted or hazardous areas)?
	4. Have local first responders participated in exercises and / or trainings?
10. How does your organization handle emergency communication?
	1. Are critical telephone calls getting through to the United States? If not, is there an alternate means of communication available?
	2. How will the ship’s crew interact with local media representatives and control media access to the ship / port?
	3. Are there procedures to manage the media when they arrive?
	4. Are there procedures to manage social media posts about the incident before giving an official statement?
11. Does the ship maintain security technology that can assist law enforcement in response efforts?
	1. Can security personnel assist in locating victims and assailants via closed-circuit television or similar capabilities?
	2. Are there access control capabilities on the ship to facilitate entry of first responders, prevent entry to visitors or additional employees, and manage contractors on-site?
	3. Can the ship remotely control access to critical components or activate / deactivate card readers, including the capability to deactivate a specific card?
	4. Is there sufficient emergency lighting capability on the ship to deal with a nighttime incident?
12. Do the ship’s incident response plans cover the emergency coordination activities described in the module?
	1. How do responders coordinate the response, and who maintains decision-making authority when management is not available?
	2. Does the security plan or any other plan outline the delegation of authority?
	3. If someone locked the doors / ramps to critical components, how does law enforcement obtain access?
	4. Have you identified a safe location for people who are evacuating the immediate area?
13. Does your organization conduct an accountability check of your employees?
14. If so, who is responsible for this? Who collects the information? What is done if an employee does not respond?
15. Do your plans and procedures outline this?

# Module Three: Recovery Phase

## Scenario

## [Insert Location]

### 3–12 hours post-incident:

At 3:00 p.m., local and international media sources begin reporting that the attack gave 16 crew members and 11 guests minor, non-life-threatening injuries. There were no fatalities. Many of the injured crew members and guests are U.S. citizens, and responders informed the FBI and U.S. Department of State.

The ship sustained substantial damage to its navigational system, and because of the extent of the damage, the ship must be kept in port until the crew can make the necessary repairs.

By 5:00 p.m., local law enforcement has created a security perimeter around the port and has swept the ship for any additional threats, though they found none. Responders transported the wounded individuals to a local hospital to undergo treatment. Local authorities are working in conjunction with on-board and shore-side security on the drone IED attack investigation.

Since there is little remaining physical evidence of the drones left at the scene of the incident, local authorities warn the investigation will take time, especially since the attackers could have stationed themselves up to three miles away from where the crew docked the ship.

Families of the victims are calling for information about their loved ones. On board, crew members have begun locating all guests—both on- and off-board—and beginning the family reunification process. Once located, Guest Relations employees have been communicating with guests outside of the port area to help them acquire accommodations until the ship’s repairs are complete. Videos and rumors about the attack are running rampant on social media.

Shore-side personnel have notified the ship that they are in route to the port to begin repairs and further investigate.

At 11:30 p.m., the radical group, [insert group name], claimed responsibility for the drone attack on their social media pages. They stated their intent was to continue paralyzing cruise line operations “one by one” until the cruise industry, in its entirety, permanently shuts down.

Following these events, [Enter company name] has released an official media statement about the incident.

## Discussion Questions

1. What are the response priorities at this stage of short-term recovery?
2. How do you determine the status of your facilities before, during, and after an incident?
3. How does your organization track patients?
	1. Who is responsible for tracking patients?
	2. What are you telling the families of victims?
4. How does your organization reunite guests separated from their families?
	1. Does your organization have specific procedures regarding family reunification? If so, what are they?
	2. What local facilities and resources can your organization leverage for family reunification efforts?
	3. What communication procedures are taking place if the attack separated people?
		1. How is your organization contacting separated families?
	4. Is there a specific area where family reunification can take place on board?
		1. Where is it?
		2. Who is responsible for managing the reunification process?
5. What are the established procedures to locate guests ashore during an emergency?
	1. Who is responsible for locating guests?
	2. What are the protocols for getting them back on board?
6. How do current ship / company emergency plans address the coordination of local emergency response personnel at this point in the incident?
7. How does law enforcement determine that the scene is clear and free of all IEDs?
8. How will the ship address any impediments to local authorities’ operations / investigations?
	1. How will your organization coordinate personnel accountability and communication?
		1. Who makes a list of the injured?
		2. Once [insert appropriate decision making organization(s)] gives an all clear, how does your organization communicate that information to any passengers or crew sheltered-in-place?
	2. Where are the pre-determined locations for the command post and staging area(s)?
	3. Is there a process to assist law enforcement with victim identification? Are the protocols different for passengers versus crew?
9. Are there protocols to understand who has legal jurisdiction in the aftermath of such an incident?
10. What are the plans to handle the significant media attention from national and international outlets?
	1. Are there separate plans to handle social media?
	2. What training do crew members receive regarding media relations and the release of sensitive information?
	3. How would the company handle social media posts and public messaging in the aftermath of such an occurrence?
11. What information sharing protocols exist for guests and crew members?
	1. What information about this attack would shore-side security share with other ships in their company?
	2. What mechanisms would crew use to relay relevant information to local authorities?
	3. How would the crew receive information about the incident?
		1. How would guests receive information about the incident?
	4. What information on the incident would shore-side personnel share with the families of injured passengers and crew members, and how would this be done?
12. Is there a business continuity or rapid recovery plan that addresses an IED incident?
	1. What are the plans for the passengers and crew members unable to enter the ship because of the investigation?
		1. How will the company handle communications with passengers, and will there be a reimbursement plan?
		2. How will the ship address any impediments to operations?
		3. Can law enforcement estimate the timeframe required to consider the ship a crime scene?
	2. What are the ship’s priorities related to continuity and recovery?
	3. Are there any potential liability issues from this incident that ship personnel would be addressing at this point?
13. What victim assistance is available for crew members following this incident? And for passengers?
	1. How does your organization communicate information with crew members and their families following the incident?
	2. Will counseling for crew members and guests be available?
	3. Will there be any financial assistance or benefit programs for crew members if you must shut down the ship temporarily?
	4. Are there restitution benefits for injured guests? If so, what are they?
	5. What is the procedure if injuries received on the job (in this case by an IED) hospitalized an employee?

This page is intentionally left blank.

# Appendix A: Exercise Participants

| **Participating Private Sector Organizations** |
| --- |
| [Insert private sector participants] |
|  |
|  |
|  |

| **Participating Local Organizations** |
| --- |
| [Insert local participants] |
|  |
|  |
|  |

| **Participating State Organizations** |
| --- |
| [Insert state participants] |
|  |
|  |
|  |

| **Participating Federal Organizations** |
| --- |
| [Insert federal participants] |
|  |
|  |
|  |

|  |
| --- |
| **Other Participating Organizations**  |
| [Insert other participants] |
|  |
|  |
|  |

This page is intentionally left blank.

# Appendix B: Relevant Plans

[Insert excerpts from relevant plans, policies, or procedures to be tested during the exercise.]

This page is intentionally left blank.

# Appendix C: Acronyms

| Acronym | Term |
| --- | --- |
| **AAR** | After-Action Report |
| **CBP** | Customs and Border Protection |
| **CISA** | Cybersecurity and Infrastructure Security Agency |
| **CTEP** | CISA Tabletop Exercise Package |
| **DHS** | Department of Homeland Security |
| **EPT** | Exercise Planning Team |
| **FBI** | Federal Bureau of Investigation |
| **HSIN**–**CI** | Homeland Security Information Network – Critical Infrastructure |
| **IED** | Improvised Explosive Device |
| **IP** | Improvement Plan |
| **PA** | Public Address  |
| **POC** | Point of Contact |
| **PSA** | Protective Security Advisor |
| **SitMan** | Situation Manual |
| **SME** | Subject Matter Expert |
| **TTX** | Tabletop Exercise |
| **USSS** | U.S. Secret Service |

